Microsoft®

Windows® 2000

Server Operating System

IP Security for Microsoft Windows 2000 Server

White Paper

Abstract

The Microsoft® Windows® 2000 Server operating system includes an implementation of the Internet Engineering Task Force's IP Security Protocol. Windows IP Security provides network managers with a key line of defense in protecting their networks. Windows IP Security exists below the transport level, so its security services are transparently inherited by applications. Upgrading to Windows 2000 Server provides the protections of integrity, authentication, and confidentiality without having to upgrade applications or train users.

© 1999 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, the BackOffice logo, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0299

CONTENTS

INTRODUCTION....1

BENEFITING FROM IP SECURITY....3
Building Upon IP Security 3
Full Support of Industry Standards 3
Diffie-Hellman (DH) Technique 4
Hash Message Authentication Code (HMAC) 4
HMAC-MD5 4
HMAC-SHA 4
DES-CBC 4
Supported Standards and References 4
Flexible Security Protocols 4
Internet Security Association and Key Management Protocol 5
Oakley 5
IP Authentication Header 5
IP Encapsulating Security Protocol 5
Cost Savings 5
Software Upgrades 5
Training 5
Cryptographic Key Management 6

DEPLOYING WINDOWS IP SECURITY....7
Evaluate Information 7
Create Scenarios 7
Determine Required Security Levels 7
Build Security Policies with Security Manager 7
Flexible Security Policies 7
Flexible Negotiation Policies 8
Filters 8
Creating a Security Policy 8
Diagramming a Basic Deployment 9
Compatibility Notes 10

SUMMARY....12

FOR MORE INFORMATION....13

INTRODUCTION

The Microsoft® Windows® 2000 Server operating system simplifies deployment and management of network security with Windows® IP Security, a robust implementation of the IP Security Protocol (IPSec).

The need for Internet Protocol (IP)-based network security is already great and growing. In today's massively interconnected business world of the Internet, intranets, branch offices, and remote access, sensitive information constantly crosses the networks. The challenge for network administrators and other IS professionals is to ensure that this traffic is:

- Safe from data modification while en route.
- Safe from interception, viewing or copying.
- Safe from being accessed by unauthenticated parties.

These issues are known as data integrity, confidentiality, and authentication. In addition, replay protection prevents acceptance of a resent packet.

Designed by the Internet Engineering Task Force (IETF) for the Internet Protocol, IPSec supports network-level authentication, data integrity and encryption. IPSec integrates with the inherent security of the Windows 2000 Server operating system to provide the ideal platform for safeguarding intranet and Internet communications.

Microsoft Windows IP Security uses industry-standard encryption algorithms and a comprehensive security management approach to provide security for all TCP/IP communications on both sides of an organization's firewall. The result is a Windows 2000 Server end-to-end security strategy that defends against both external and internal attacks.

And because Windows IP Security is deployed below the transport level, network managers (and software vendors) are spared the hassle and expense of trying to deploy and coordinate security one application at a time. By simply deploying Windows 2000 Server, network managers provide a strong layer of protection for the entire network, with applications automatically inheriting the safeguards of Windows 2000 Server security. The encryption support of Windows IP Security extends to Virtual Private Networks (VPNs) as well.

Network administrators and managers benefit from integration of IPSec with Windows 2000 Server for a number of reasons, including:

- **Open Industry Standard**—IPSec provides an open industry-standard alternative to proprietary IP encryption technologies. Network managers benefit from the resulting interoperability.
- **Transparent—**IPSec exists below the transport layer, making it transparent to applications and users, meaning there is no need to change network applications on a user's desktop when IPSec is implemented in the firewall or router.

BENEFITING FROM IP SECURITY

- **Authentication—**Strong authentication services prevent the interception of data by using falsely claimed identities.
- **Confidentiality—**Confidentiality services prevent unauthorized access to sensitive data as it passes between communicating parties.
- **Data Integrity—**IP Authentication Headers and variations of Hash Message Authentication Code ensure data integrity during communications.
- **Dynamic Rekeying—**Dynamic rekeying during ongoing communications helps protect against attacks.
- **Secure Links End-to-End—**Windows IP Security provides secure links end-to-end for private network users within the same domain or across any trusted domain in the enterprise.
- **Centralized Management—**Network administrators use security policies and filters to provide appropriate levels of security based on user, work group, or other criteria. Centralized management reduces administrative overhead costs.
- **Flexibility—**The flexibility of Windows IP Security allows policies to apply enterprise-wide, or to a single workstation.

All of this is good news to network managers and other IS professionals charged with protecting the security of information. The explosive growth of intranets, and the increasing integration of corporate networks with the Internet, have caused an even greater need for security. And although the classic security concern is to protect data from outsiders, Windows IP Security also provides protection against attacks from what is the more likely source—unauthorized access by insiders.

Whether setting security profiles for key workgroups or the entire network, the encryption support of Windows IP Security can provide network managers with the peace of mind that comes from protecting an enterprise’s communications.

Most network security strategies have focused on preventing attacks from outside the organization’s network. Firewalls, secure routers, and token authentication of dial-up access are examples of management attempts to defend against external threats. But hardening a network’s perimeter does nothing to protect against attacks mounted from within.

In fact, an organization can lose a great deal of sensitive information from internal attacks mounted by employees, supporting staff members, or contractors. And firewalls offer no protection against such internal threats.

One of the great benefits of Windows 2000 Server integration with IP Security is the ability to protect against both internal and external

attacks. And, again, this is done transparently, imposing no effort or additional overhead on individual users.

Building Upon IP Security

IP Security as defined by the Internet Engineering Task Force uses an Authentication Header (AH) and an Encapsulated Security Payload (ESP). The Authentication Header provides data communication with source authentication and integrity. The Encapsulated Security Payload provides confidentiality in addition to authentication and integrity. With IP Security, only the sender and recipient know the security key. If the authentication data is valid, the recipient knows that the communication came from the sender, and that it was not changed in transit.

Windows IP Security builds upon the IETF model by mixing public key and secret key cryptography, and by providing automatic key management for maximized security and high-speed throughput. This gives a combination of authentication, integrity, antireplay, and (optionally) confidentiality, to ensure secure communications. Since Windows IP Security is below the network layer, it is transparent to users and existing applications. Organizations automatically get high levels of network security.

Windows IP Security features include:

- Full Support of Industry (IETF) Standards
- Flexible Security Protocols
- Easy Implementation and Management
- Flexible Security Policies
- Flexible Negotiation Policies
- Cost Savings

Full Support of Industry Standards

Windows 2000 makes full use of powerful, industry-standard cryptographic algorithms and authentication techniques. These include:

- Diffie-Hellman Technique to agree upon a shared key.
- Hash Message Authentication Code (HMAC) and variations, to provide integrity and antireplay.
- Data Encryption Standard−Cipher Block Chaining for confidentiality.

Diffie-Hellman (DH) Technique

The Diffie-Hellman Technique (named for its inventors Whitfield Diffie and Martin Hellman) is a public key cryptography algorithm that allows two communicating entities to agree on a shared key. Diffie-Hellman starts with the two entities exchanging public information. Each entity then combines the other's public information along with its own secret information to generate a shared-secret value.

Hash Message Authentication Code (HMAC)

HMAC is a secret-key algorithm providing integrity and authentication. Authentication using keyed hash produces a digital signature for the packet that can be verified by the receiver. If the message should change in transit, the hash value will be different and the IP packet will be rejected.

HMAC-MD5

Message Digest function 95 (MD5) is a hash function that produces a 128-bit value.

HMAC-SHA

Secure Hash Algorithm (SHA) is a hash function that produces a 160-bit value. While a bit slower than HMAC-MD5, HMAC-SHA is more secure.

DES-CBC

Data Encryption Standard (DES) - Cipher Block Chaining (CBC) is a secret key algorithm used for confidentiality. A random number is generated and used with the secret key to encrypt the data.

Supported Standards and References

Windows 2000 fully supports and employs protocols published by the Internet Engineering Task Force. The implementation is compliant with the latest IETF drafts proposed in the IPSec working group, including the overall architecture documents and documents pertaining to header formats and transforms, in addition to ISAKMP/Oakley drafts.

Windows 2000 IP Security implements Internet Security Association and Key Management Protocol (ISAKMP) using Oakley key determination protocol, which allows for dynamic rekeying.

Flexible Security Protocols

Security protocols perform various services for secure network communications. Windows 2000 uses the following security protocols:

- Internet Security Association and Key Management Protocol
- Oakley Key Determination
- IP Authentication Header
- IP Encapsulating Security Protocol

Internet Security Association and Key Management Protocol

Before IP packets can be transmitted from one computer to another, a Security Association (SA) must be established. An SA is a set of parameters that defines the services and mechanisms necessary, such as keys, to protect communications for a security protocol. An SA must exist

between the two communicating parties using IP Security. Internet Security Association and Key Management Protocol (ISAKMP) defines a common framework to support the establishment of security associations. ISAKMP is not linked to one specific algorithm, key generation method, or security protocol.

Oakley

Oakley is a key determination protocol, which uses the Diffie-Hellman key exchange algorithm. Oakley supports Perfect Forward Secrecy (PFS), which ensures that if a single key is compromised, it will permit access only to data protected by a single key. It never reuses the key that protects communications to compute additional keys, and never uses the original key generation material to compute another key.

IP Authentication Header

IP Authentication Header (AH) provides integrity, authentication, and antireplay. Confidentiality is not a property of AH. AH uses an algorithm to compute a keyed message hash (an HMAC) for each IP packet.

IP Encapsulating Security Protocol

In addition to the AH services listed above, IP Encapsulating Security Protocol (ESP) provides confidentiality using the DES-CBC algorithm.

Cost Savings

Historically, organizations have had to strike a difficult balance between the desire to protect their data communications, and the high costs of establishing and maintaining that protection. Security can impose costs that exceed the hardware cost of the network. These costs have fallen into the following categories:

- Software Upgrades
- Training
- Key Management

Software Upgrades

Because Windows IP Security is deployed at the transport level, it is transparent to existing software applications. With Windows IP Security providing security for the network, applications inherit this security, and no application modifications are needed. Network-level security provides for immense savings by eliminating the need to upgrade applications.

Training

Because Windows 2000 IP Security is transparent to users, no user training is required, and this expense is eliminated.

DEPLOYING WINDOWS IP SECURITY

Cryptographic Key Management

To provide security, cryptographic keys must be changed regularly. When a system administrator has to do this manually, key management becomes extremely time consuming. Either the keys are not changed as frequently as the organization may want, or they are changed on a few vital machines. Windows IP Security automatically handles key management. The costs of manually changing keys are eliminated, and maximum protection can be established and maintained across the enterprise.

Microsoft 2000 Server has been designed to provide very high levels of data security coupled with ease of implementation and administration. The result is enterprise-wide information security at low total cost-of-ownership levels. Windows 2000 Server gives great flexibility with security, user, and domain policies. The network administrator can apply policies enterprise-wide, or down to a single user or workstation. Security policies can then be implemented transparently, with no further intervention required from the network administrator, and no retraining of users.

To establish security, a network administrator goes through a four-step process:

- Evaluate information sent over the network and the Internet.
- Create communication scenarios.
- Determine security levels required for each scenario.
- Build security policies using Windows Security Manager.

Evaluate Information

All information sent over networks or over the Internet is subject to interception, examination, or modification. A system administrator can determine which kinds of information are most valuable, and what communication scenarios are most vulnerable.

Create Scenarios

Organizations have certain patterns to their information flows. A system administrator can determine these predictable patterns. For example, remote sales offices will send projected sales data, purchase orders, and other financial information to the home office. Each of these communication scenarios can have different IP Security policies. A system administrator might also decide, for example, that all communications with the human resources department should be secure.

Determine Required Security Levels

The required security levels will change, depending upon the sensitivity of the information, and the relative vulnerability of the transmission carrier. Windows 2000 Security Manager lets a network administrator quickly and easily set the appropriate level of security.

Build Security Policies with Security Manager

Windows 2000 Server Security Manager lets a network administrator set security algorithms, and assign them to groups of computers or single computers. Policies are built and assigned using fast point-and-click operations.

Flexible Security Policies

Each configuration of Windows IP Security attributes is called a Security Policy. Security Policies are built on associated Negotiation Policies and IP Filters. An IP Security Policy can be assigned to the Default Domain Policy, the Default Local Policy, or a customized policy you create. The computers in the domain will automatically pick up the properties of the Default Domain and Default Local policies, including the IP Security Policy assigned to that domain policy.

Flexible Negotiation Policies

Negotiation policies determine the security services you want to include for each type of communication scenario you envision for the enterprise. A network administrator can choose between services that include confidentiality or those that do not. The administrator can set multiple security methods for each negotiation policy. If the first method is not acceptable for the security association, the ISAKMP/Oakley service will continue down the list until it finds one it can use to establish the association.

Filters

Filtering allows Windows 2000 Server to apply different security policies to different machines. IP filters determine which actions to take based upon the destination and protocol of individual IP packets.

Creating a Security Policy

An example of creating a security policy could be found in an organization with a centralized legal department. The network administrators could decide that communications within the department had to be secure, but not confidential. However, the administrator could decide that communications between the Legal Department and other

departments within the organization must be both secure and confidential. Windows IP Security allows filtering to apply the appropriate security policy to communication initiated within the Legal Department. If the communication destination is outside the department, Windows IP Security applies a security policy that provides security and confidentiality. If the packet is simply moving to another destination within the Legal Department, security is applied, but without confidentiality.

To implement the security plan for the Legal Department, the administrator would take the following steps:

1. Create a security policy called “Legal” and assign it to the Default Domain policy. As each computer in the company logs on to the domain, the computer’s Policy Agent would pick up the Legal Department security policy from the directory service. The Legal Department security policy would have the following negotiation policies and IP filters associated with it:
2. Create two negotiation policies and associate with the Legal Department security policy:

   The first negotiation policy, Legal NP 1, is set to a service that provides confidentiality when users in the Legal Department are communicating with non-Legal Department users (“Transferred data will be Confidential, Authentic and Unmodified”: ESP security protocol).

   The second negotiation policy, Legal NP 2, is set to a service that only provides authentication and protection against modification when Legal Department users are communicating with each other (“Transferred data will be Authentic and Unmodified”: AH security protocol).

3. Create two IP Filters and associate each with a negotiation policy: The users in the Legal Department are on network 157.55.0.0 with a subnet mask of 255.255.0.0. The non-Legal Department users are on network 147.20.0.0 with a subnet mask of 255.255.0.0. The first IP filter, Legal IP Filter 1, is for users in the Legal Department who communicate to non-Legal Department users. It will be associated with negotiation policy Legal NP1. The administrator sets the filter properties to the following values:

   The specified IP address for the source (sender of data) is 157.55.0.0. This address will match any IP address in the Legal Department’s network, since it is really an IP subnet address.

   The specified IP address for the destination (receiver of data) is 147.20.0.0.

Since the company’s security plan stipulates protecting all data sent over the IP protocol, the protocol type is Any.

Legal Department users communicating to other users within the Department will use the second IP filter, Legal IP Filter 2. It is associated with negotiation policy Legal NP 2, and the filter properties are set to the following values:

- The specified IP address for the source (sender of data) is 157.55.0.0.
- The specified IP address for the destination (receiver of data) is 157.55.0.0.
- The protocol type is set to Any.

When a user in the Legal Department sends information to any other user, the source and destination addresses of the IP packets are checked against the IP filters in the Legal security policy. If the addresses match one of the filters, the associated negotiation policy determines the level of IP Security for the communication.

For example, if a user in the Legal Department with an IP address of 157.55.2.1 sends data to a user at 147.20.4.5, this would match Legal IP Filter 2. This would mean the communication is sent at the security level specified by the negotiation policy Legal NP1, which provides authentication and protection against modification (unmodified) and confidentiality during the communication.

Diagramming a Basic Deployment

In the example below, a user on Host A is sending data to a user on Host B. Windows IP Security has been implemented for both computers.

At the user level, the process of securing the IP packets is transparent. User 1 simply launches an application that uses the TCP/IP protocol, such as FTP, and sends the data to User 2.

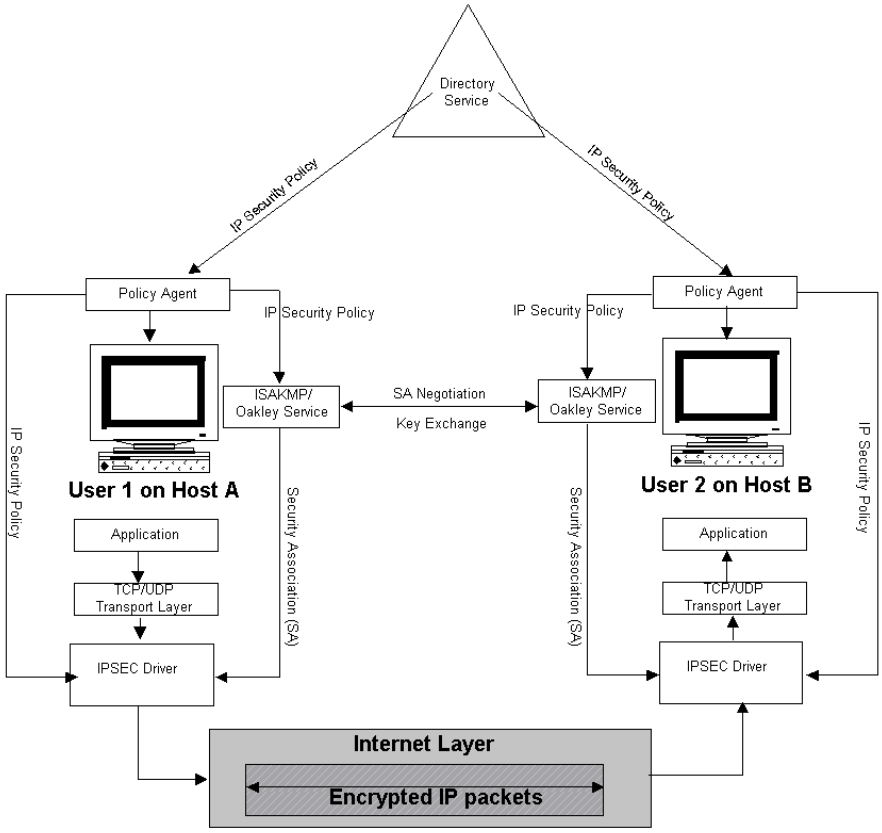

Figure 2. Example of a Windows IP Security deployment.

The security policies assigned to Host A and Host B by the administrator determine the level of security for the communication. These are picked up by the Policy Agent and passed to the ISAKMP/Oakley service and IPSEC driver. The ISAKMP/Oakley service on each computer uses the negotiation policies associated with the assigned security policy to establish the key and a common negotiation method (a security association). The results of the ISAKMP policy negotiation between the two computers are passed to the IPSEC driver, which uses the key to encrypt the data. Finally, the IPSEC driver sends the encrypted data to Host B. The IPSEC driver on Host B decrypts the data and passes it up to the receiving application.

Compatibility Notes

To ensure full communications compatibility with Windows 9x and earlier versions of Windows NT, a computer running Windows 2000 configured for IP Security will send the data without encryption to a computer not running Windows 2000.

Any routers or switches that are in the path between the communicating hosts, whether two users or a user and a file server, should simply

forward the encrypted IP packets through toward their destination. If a firewall or other security gateway is between the communicating hosts, IP forwarding or special filtering that permits forwarding for IP Security Packets must be enabled for the IP packets to reach their destination correctly.

The Windows IP Security integrated into Windows 2000 Server provides network managers with a critically important line of security. And because Windows IP Security is deployed below the transport level, deploying security has never been easier. Upgrading to Windows 2000 Server provides the protections of integrity, authentication, and confidentiality without having to upgrade applications or train users.

Windows IP Security is an implementation of the Internet Engineering Task Force's IP Security Protocol, assuring maximum interoperability with IPSec solutions deployed on other networks.

The flexibility and centralized management makes Windows IP Security easy to administer, with network managers able to create custom security policies and filters based on user, work group, or other criteria.

The end-to-end security ensures that data sent over any network—whether LAN, WAN, or Internet—maintains integrity and secrecy in transit; it also ensures that data can only be accessed by authenticated users.

At a time when network security is increasingly vital, Windows 2000 Server makes it easy for network managers to provide a strong layer of protection to their organization's information resources.

For the latest information on Windows 2000 Server, check out our World Wide Web site at http://www.microsoft.com/ntserver or the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest IETF IPSec drafts, go to:

www.ietf.org/html.charters/ipsec-charter.html